



Identity and Smart Card Technology and Application Glossary

April 2007

Developed by:
Smart Card Alliance Identity Council

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.

The Smart Card Alliance Identity Council is focused on promoting the need for technologies, legislation, and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud, and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Additional information about the use of smart cards for secure identity and payment applications can be found at <http://www.smartcardalliance.org>.

Copyright © 2007 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Identity and Smart Card Technology and Application Glossary

This glossary was developed by the Smart Card Alliance Identity Council to define commonly used terms related to identity and smart card technology and applications.

3DES

See Triple DES

A

Access control

The process of granting or denying specific requests to: 1) obtain and use information and related to information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Access control system format

The algorithm that specifies how data transmitted by the system is to be interpreted. The format specifies how many bits make up the data stream and which bits represent different types of information. For example, the first few bits might transmit the facility code, the next few the unique ID number, the next few parity, and so on.

Access management

The processes and technologies for controlling and monitoring access privileges to resources, consistent with governing policies. Access management includes authentication, authorization, trust, and security auditing.

Access right

The privilege or permission for an individual to access a controlled resource or entity (physical or logical).

AES

Advanced Encryption Standard (AES), also known as Rijndael. A block cipher adopted as an encryption standard by the U.S. government.

API

See application programming interface.

Applicant

An individual applying for an identity card/credential. In context of the Federal Personal Identity Verification (PIV) card, the applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.

Application

A hardware/software system implemented to satisfy a particular set of requirements. In the context of FIPS 201, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Application authority

The entity that defines the rules of the application and attribute disclosure required from a subject to be disclosed in order to provide the service which may be delegated to a service provider.

Application programming interface (API)

A source code interface that a computer system or program library provides in order to support requests for services to be made of it by other computer programs, and/or to allow data to be exchanged.

Asymmetric cryptographic technique

A cryptographic technique that uses two related operations: a public operation defined by public numbers or by a public key and a private operation defined by private numbers or by a private key. (The two operations have the property that, given the public operation, it is computationally infeasible to derive the private operation.)

Asymmetric keys

Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Assurance level

The degree of certainty that the user has presented an identifier (e.g., a credential) that refers to his or her identity. In the context of FIPS 201, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Attribute

A quality, characteristic or entity that defines properties of a subject (e.g., person), object or element.

Authenticate

To verify (guarantee) the identity of a person or entity. To ensure that the individual or organization is really who it says it is.

Authentication

The process of validating the identity of a person or other entity.

Authentication factors

Pieces of information used to verify a person's identity for security purposes. The three most commonly recognized factors are:

- Something you know, such as a password or personal identification number (PIN)
- Something you have, such as a credential, card or token
- Something you are, such as a fingerprint or other biometric.

Authorization

The assignment of a privilege or privileges (e.g., access to a building or network) verifying that a known person or entity has the authority to perform a specific operation. Authorization is provided after authentication.

B**Biometric**

A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Biometric data

Data encoding a feature or features used in biometric verification.

Biometric information

The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

Biometric reference data

Data stored on the card for the purpose of comparison with the biometric verification data.

Biometric system

An automated system capable of the following:

- Capturing a biometric sample from an end user
- Extracting biometric data from that sample
- Comparing the extracted biometric data with data contained in one or more references
- Deciding how well they match
- Indicating whether or not an identification or verification of identity has been achieved

Biometric template

The formatted digital record used to store an individual's biometric attributes. This record typically is a translation of the individual's biometric attributes and is created using a specific algorithm.

Biometric verification

The process of verifying, using a one-to-one comparison, the biometric verification data against biometric reference data.

Breeder document

A document used as an original source of identity to apply for (or breed) other forms of identity credentials.

C**Capture**

The method of taking a biometric sample from an end user.

Card

- a. A type of physical form factor designed to carry electronic information and/or human readable data.
- b. Under FIPS 201, a dual interface smart card-based ID badge for both physical and logical access that contains within it an integrated circuit chip.

Card issuer

The organization or entity that issues cards.

Card management system (CMS)

A smart card/token and digital credential management solution that is used to issue, manage, personalize and support cryptographic smart cards and PKI certificates for identity-based applications throughout an organization.

Card reader

Any device that reads encoded information from a card, token, or other identity device and communicates to a host such as a control panel/processor or database for further action.

Card serial number

An identifier which is guaranteed to be unique among all identifiers used for a specific purpose (see unique identifier).

Cardholder

An individual to whom an ID card is issued or assigned.

Certificate

See digital certificate.

Certificate authority (CA)

A trusted third party that is responsible for issuing and revoking digital certificates within the public key infrastructure.

Certificate revocation list (CRL)

A list of certificates that have been revoked before their expiration by a certificate authority.

Certification

The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Chain of trust

An attribute of a secure ID system that encompasses all of the system's components and processes and assures that the system as a whole is worthy of trust. A chain of trust should guarantee the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust must also ensure that information within the system is verified, authenticated, protected, and used appropriately.

Challenge

The demand for disclosure of one or more attributes related to a subject made by service authority.

Challenge/response

A family of protocols in which one party (e.g., a reader) presents a question ("challenge") and another party (e.g., a credential) must provide a valid answer ("response") in order to be authenticated.

Checksum

A computed value that depends on the contents of a message. The checksum is transmitted with the message. The receiving party can then recompute the checksum to verify that the message was not corrupted during transmission.

Chip

Electronic component that performs logic, processing and/or memory functions.

CHUID

Cardholder Unique Identifier. Part of the standardized data model for cardholder identification data for FIPS 201.

Claim

An assertion by a subject about the value of an attribute.

Cloning

The process of creating an identical copy of something.

Component

An element of a larger system. In the FIPS 201 context, a component can be an identity card, PIV issuer, PIV registrar, card reader, or identity verification support, within the PIV system.

Confidence level

The degree of likelihood that an identifier refers to a specific individual.

Contact smart card

A smart card that connects to the reading device through direct physical contact between the smart card chip and the smart card reader. (See ISO/IEC 7816.)

Contactless smart card

A smart card that communicates with a reader through a radio frequency interface.

Control panel

The access control system component that connects to all door readers, door locks and the access control server. The control panel validates the reader and accepts data. Depending on the overall system design, the control panel may next send the data to the access control server or may have

enough local intelligence to determine the user's rights and make the final access authorization. The control panel can be called the controller or panel.

Control point

Any device which is controlled by a physical access system (for example, doors, turnstiles, gates, lights, cameras, elevators). There may be multiple control points for a single access requirement.

Credential

- a. Evidence attesting to one's rights, privileges or evidence of authority.
- b. In FIPS 201, the PIV card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. A smart card can store multiple digital credentials.

Cryptographic key

See key.

Cryptographic smart cards

Advanced smart cards that are equipped with specialized cryptographic hardware that lets algorithms such as RSA be used on the card. Today's cryptographic smart cards are also able to generate key pairs on the card, to avoid the risk of having more than one copy of the key (since by design (usually) there isn't a way to extract the keys from a smart card). Cryptographic smart cards are often used for digital signatures and secure identification.

D

Data integrity

The condition in which data is identically maintained during any operation, such as transfer, storage, and retrieval.

DES

Data Encryption Standard. A method for encrypting information. (See related term Triple DES.)

Digital certificate (or public key certificate)

Digital documents (e.g., information such as the name of the person or an organization and their address) attesting to the binding of a public key to an individual or other entity. Digital certificates allow verification of the claim that a specific public key does in fact belong to a specific individual.

Digital signature

Digital information used for the purpose of identification of an electronic message or documents. Digital signatures provide a way of authenticating the identity of creators or producers of digital information.

Discretionary access control (DAC)

Access restriction based solely on an individual's identity.

Door reader

The device on each door that communicates with a card or credential and sends data from the card to the controller for decision on access rights.

Door strike

The electronic lock on each door that is connected to the controller.

DSA

Digital Signature Algorithm.

Dual interface card

A smart card that has a single smart card chip with two interfaces -- a contact and a contactless interface -- using shared memory and chip resources.

E

Eavesdropping

The interception of communications between a reader and a credential during transmission by unintended recipients. Messages can be protected against eavesdropping by employing a security service usually implemented by encryption.

ECC

Elliptic Curve Cryptography

EMV

Europay MasterCard Visa. Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals.

Encryption

The process of translating information into a code that can only be read if the reader has access to the key that was used to encrypt it. There are two main types of encryption -- asymmetric (or public key) and symmetric (or secret key).

End point products

As defined in NIST SP 800-73, products that employ a unified card edge interface that is technology independent and compliant with current international standards.

Enrollment

The process of entering the appropriate identity data for an individual into a system and associating the identity with the privileges being granted by the system.

Enterprise single sign-on (ESSO)

A system designed to minimize the number of times that a user must type their ID and password to sign into multiple applications. The E-SSO solution automatically logs users in and acts as a password filler where automatic login is not possible. Each client is typically given a token that handles the authentication; in other E-SSO solutions each client has E-SSO software stored on their computer to handle the authentication. An E-SSO authentication server is also typically implemented into the enterprise network.

ePassport

A travel document that contains an integrated circuit chip based on international standard ISO/IEC 14443 and that can securely store and communicate the ePassport holder's personal information to authorized reading devices.

EPC Generation 2 (EPC Gen 2)

The specification developed by EPCglobal for the second-generation RFID air-interface protocol. EPC Gen 2 was developed to support supply chain applications (e.g., tracking inventory). The current ratified standard operates in the ultra-high-frequency (UHF) range (860-960 MHz), supports operation at long distances (e.g., 25-30 feet), and has minimal support for security (e.g., static passwords to access or kill information on the RFID device).

EPCglobal

The not-for-profit organization establishing and supporting "the EPCglobal Network™ as the global standard for real-time, automatic identification of information in the supply chain of any company, anywhere in the world" and "leading the development of industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID) in today's fast-moving, information rich, trading networks." Additional information can be found at <http://www.epcglobalinc.org>.

Excite field

The RF field or electromagnetic field constantly transmitted by a contactless door reader. When a contactless card is within range of the excite field, the internal antenna on the card converts the field energy into electricity that powers the chip. The chip then uses the antenna to transmit data to the reader.

F**Fair Information Practices**

The basis for privacy best practices, both online and offline. The Practices originated in the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. government. The Fair Information Practices include notice, choice, access, onward transfer, security, data integrity, and remedy.

Faraday cage

An enclosure formed by conducting material, or by a mesh of such material, that blocks out external static electrical fields. Any electric field will cause the charges to rearrange so as to completely cancel the field's (RF signal) effects in the cage's interior.

FASC-N

Federal Agency Smart Credential Number. The data element that is the main identifier on the PIV card and that is used by a physical access control system.

Federal Information Processing Standard (FIPS)

A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS publication covers some topic in information technology to achieve a minimum level of quality or interoperability.

Federated identity

In information technology (IT), federated identity has two general meanings:

- a. The virtual reunion, or assembled identity, of a person's user information (or principal), stored across multiple distinct identity management systems. Data is joined together by use of the common token, usually the user name.
- b. The process of a user's authentication across multiple IT systems or even organizations.

FIPS 201

Federal Information Processing Standard Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

Form factor

The physical device that contains the smart card chip. Smart chip-based devices can come in a variety of form factors, including plastic cards, key fobs, wristbands, wristwatches, PDAs, and mobile phones.

G**Gramm-Leach-Bliley**

The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act), enacted to facilitate affiliation among banks, securities firms, and insurance companies. The Act includes provisions to protect consumers' personal financial information held by financial institutions.

GSM

Global System for Mobile Communications

H

Hacking

The act of gaining illegal or unauthorized access to a computer system or network.

Hash algorithm

A software algorithm that computes a value (hash) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

Head-end system

The physical access control server, software and database(s) used in a physical access control system.

High frequency (HF)

Radio frequencies (RF) in the range of 3 MHz to 30 MHz. When used in an RF-based identification system, the high frequency used is typically 13.56 MHz.

HIPAA

Health Insurance Portability and Accountability Act of 1996. HIPAA was passed to protect health insurance coverage for workers and their families and to encourage the development of a health information system by establishing standards and requirements for the secure electronic transmission of certain health information. HIPAA mandates that the design and implementation of the electronic systems guarantee the privacy and security of patient information gathered as part of providing health care.

HSPD-12

Homeland Security Presidential Directive 12. The primary objective of HSPD-12 is the development and deployment of a Federal government-wide common and reliable identification verification system that will be interoperable among all government agencies and serve as the basis for reciprocity among those agencies.

Hybrid card

A smart card that contains two smart card chips -- both contact and contactless chips -- that are not interconnected.

I

IAB

Government Smart Card Interagency Advisory Board.

ICC

Integrated circuit card. ICC typically refers to a plastic (or other material) card containing an integrated circuit which is compatible to ISO/IEC 7816.

Identification

- a. The process of using claimed or observed attributes of an entity to deduce who the entity is.
- b. The evidence of identity or fact of proof showing the attributes of the individual presenting the identification.

Identification card

Card identifying its holder and issuer which may carry data required as input for the intended use of the card and for transactions based thereon.

Identifier

Unique data used to represent a person's identity and associated attributes. Names and card numbers are examples of identifiers.

Identity

The subset of physical and/or behavioral characteristics by which an individual is uniquely recognizable. Identity is information concerning the person, not the actual person.

Identity and access management (IAM)

The combination of processes, technologies, and policies to manage digital identities and specify how digital identities are used to access resources.

Identity data

The data associated with an individual's identity within a specific system and used by that system to verify the individual's identity.

Identity document

A piece of documentation designed to verify aspects of a person's identity. (See also breeder document.)

Identity management

In information systems, the management of the identity life cycle of entities. Identity management is sometimes used in conjunction with authorization in the IT industry. Within the life cycle:

- The identity is established: a name (or number) is connected to the subject.
- The identity is re-established: a new or additional name (or number) is connected to the subject.
- The identity is described: one or more attributes which are applicable to this particular subject may be assigned to the identity.
- The identity is newly described: one or more attributes which are applicable to this particular subject may be changed.
- The identity is destroyed.

Identity management system (IDMS)

System composed of one or more computer systems or applications that manage the identity registration, verification, validation, and issuance process, as well as the provisioning and deprovisioning of identity credentials.

Identity proofing

The process of providing sufficient information (e.g., breeder documents, identity history, credentials, documents) to establish an identity to an organization that can issue identity credentials.

Identity registration

The process of making a person's identity known to a system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity theft

The appropriation of another's personal information to commit fraud, steal the person's assets, or pretend to be the person.

Identity verification

The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in an ID card or system and associated with the identity being claimed.

IEC

International Electrotechnical Commission

International Civil Aviation Organization (ICAO) MRTD

International Civil Aviation Organization Machine Readable Travel Documents. ICAO establishes international standards for travel documents. An MRTD is an international travel document (e.g., a passport or visa) containing eye- and machine-readable data. ICAO Document 9303 is the international standard for MRTDs.

Integrated circuit

Electronic component(s) designed to perform processing and/or memory functions. See chip.

Interoperability

- a. The ability of two or more systems or components to exchange information and to use the information that has been exchanged.
- b. For the purposes of FIPS 201, the ability for any government facility or information system, regardless of the PIV issuer, to verify a cardholder's identity using the credentials on the PIV card.

ISO

International Organization for Standardization

ISO/IEC 7810

The series of international standards describing the characteristics of identification cards, including physical characteristics, sizes, thickness, dimensions, construction, materials and other requirements.

ISO/IEC 7812

The governing international standard for magnetic stripe identification cards, such as door entry cards, automated teller machine (ATM) cards, and credit cards.

ISO/IEC 7816

The international standard for integrated circuit cards with contacts, as well as the command set for all smart cards.

ISO/IEC 14443

The international standard, "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards," for contactless smart chips and cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz.

ISO/IEC 15693

The international standard, "Identification Cards - Contactless Integrated Circuit(s) Cards - Vicinity Cards," for cards operating at the 13.56 MHz frequency which can be read from a greater distance as compared to proximity cards. (See ISO/IEC 14443.)

ISO/IEC 24727

A set of programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use.

Issuer (or issuing authority)

The organization that issues an identity card to an individual after identity proofing, background checks and related approvals have been completed. Typically this is an organization for which the individual is working.

K**Key**

In encryption and digital signatures, a value used in combination with a cryptographic algorithm to encrypt or decrypt data.

L**Logical access**

Access to online resources (e.g., networks, files, computers, databases).

Low frequency (LF)

Radio frequencies (RF) in the range of 30 to 300 kHz. When used in an RF-based identification system, the low frequency is typically 125 kHz.

M

Machine readable travel documents

ICAO establishes international standards for travel documents. An MRTD is an international travel document (e.g., a passport or visa) containing eye- and machine-readable data. ICAO Document 9303 is the international standard for MRTDs.

Man-in-the-middle attack

An attack on an authentication protocol in which the attacker is positioned between the individual seeking authentication and the system verifying the authentication. In this attack, the attacker attempts to intercept and alter data traveling between the parties.

Mandatory access control (MAC)

An access control technique that assigns a security level to all resources (e.g., information, parts of a building), assigns a clearance level to all potential users requiring access, and ensures that only users with the appropriate clearance level can access a requested resource.

Match/matching

The process of comparing biometric information against previously stored biometric data and scoring the level of similarity.

MCU

See microcontroller.

MD5

One of the most popular hashing algorithms, developed by Professor Ronald L. Rivest of MIT, which produces a 128-bit hash from any input.

Memory card

Typically a smart card or any pocket-sized card with an embedded integrated circuit or circuits containing non-volatile memory storage components and perhaps some specific security logic.

Message authentication code (MAC)

A short piece of information used to support authentication of a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag* or *checksum*). The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. MACs are computed and verified with the same key, unlike digital signatures.

Microcontroller (MCU)

A highly integrated computer chip that contains all of the components comprising a controller. Typically this includes a CPU, RAM, some form of ROM, I/O ports, and timers. Unlike a general purpose computer used in IT, a microcontroller is designed to operate in a restricted environment.

Microprocessor card

Typically a smart card or any pocket-sized card with an embedded integrated circuit or circuits containing memory and microprocessor components.

Model

A detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.

Multi-application card

A smart card that runs multiple applications -- for example, physical access, logical access, data storage and electronic purse -- using a single card.

Multi-factor authentication

The use of multiple techniques to authenticate an individual's identity. This usually involves combining two or more of the following: something the individual has (e.g., a card or token); something the individual knows (e.g., a password or personal identification number); something the individual is (e.g., a fingerprint or other biometric measurement).

Multi-factor reader

A smart card reader that includes a PIN pad, biometric reader, or both to allow multi-factor authentication.

Multi-technology card

An ID card that has two or more ID technologies that are independent and that don't interact or interfere with one another. An example is a card that contains a smart card chip and a magnetic stripe.

Multi-technology reader

A card reader/writer that can accommodate more than one card technology in the same reader (e.g., both ISO/IEC 14443 and ISO/IEC 15693 contactless smart card technologies or both 13.56 MHz and 125 kHz contactless technologies).

Mutual authentication

For applications requiring secure access, the process that is used for the smart card-based device to verify that the reader is authentic and to prove its own authenticity to the reader before starting a secure transaction.

N**NFC -- Near Field Communication**

A short-range wireless standard (ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they are brought close together (within 10-20 centimeters or 4-8 inches). NFC technology is compatible with ISO/IEC 14443-based technology.

NIST

National Institute of Standards and Technology

Non-repudiation

The ability to ensure and have evidence that a specific action occurred in an electronic transaction (e.g., that a message originator cannot deny sending a message or that a party in a transaction cannot deny the authenticity of their signature).

O**OCSP**

Online Certificate Status Protocol. An online protocol used to determine the status of a public key certificate.

Off-card

Refers to data that is not stored on the ID card or to a computation that is not performed by the integrated circuit on the ID card.

On-card

Refers to data that is stored on the ID card or to a computation that is performed by the integrated circuit chip on the ID card.

One-time password/OTP

Passwords that are used once and then discarded. Each time the user authenticates to a system, a different password is used, after which that password is no longer valid. The password is computed either by software on the logon computer or by OTP hardware tokens in the user's possession that are coordinated through a trusted system.

Open ID

A decentralized digital identity system, in which any user's online identity is given by, for example, a URL (such as for a blog or a home page) and can be verified by any server running the protocol. Users are able to clearly control what pieces of information can be shared such as their name, address, or phone number.

Operational range

The maximum distance between a contactless smart card reader and a contactless smart card.

P**PACS**

See physical access control system.

PAIWG

Physical Access Interagency Interoperability Working Group

Password

A form of secret authentication data that is used to control access to a resource. The password is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. Typically referred to as "something you know" for single factor authentication.

PC/SC

Personal Computer/Smart Card. The PC/SC specification defines how to integrate smart card readers and smart cards with the computing environment and how to allow multiple applications to share smart card devices.

PCSC Lite

Personal Computer/Smart Card Lite. PCSC Lite is open source software that implements the PC/SC specification for Linux.

Personal identification number (PIN)

A secret that an individual memorizes and uses to authenticate his or her identity or to unlock certain information stored on an ID card (e.g., the biometric information). PINs are generally only decimal digits.

Personal identity verification (PIV) card

The physical artifact (e.g., identity card, smart card) issued to an individual that contains printed and stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

Personally identifiable information (PII)

In information security and privacy, any piece of information which can potentially be used to uniquely identify, locate, or contact a person or steal the identity of a person.

Pharming

A cyber attack that directs people to a fraudulent website by poisoning the domain name system server.

Phishing

A cyber attack that directs people to a fraudulent website to collect personal information for identity theft.

Physical access

Access to facilities (e.g., buildings, rooms, airports, warehouses).

Physical access control system (PACS)

A system composed of hardware and software components that controls access to physical facilities (e.g., buildings, rooms, airports, warehouses).

PIN

Personal identification number. A numeric code that is associated with an ID card and that adds a second factor of authentication to the identity verification process.

PIV

See personal identity verification.

PKCS #11

Public Key Cryptography Standard #11. This standard defines the interface for cryptography operations with hardware tokens.

PKI

Public key infrastructure. See public key infrastructure.

Population

The set of users for an application.

Privacy

The ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves.

Private key

The secret part of an asymmetric key pair that is used to create digital signatures and, depending upon the algorithm, to decrypt messages, files or other information encrypted (for confidentiality) with the corresponding public key.

Privilege

An authorization or right granted by an application authority for an individual or group to perform an action.

Proximity cards

A generic name for contactless integrated circuit devices typically used for security access or payment systems. It can refer to 125 kHz RFID devices or 13.56 MHz contactless smart cards. (See ISO/IEC 14443.)

Public key

The public part of an asymmetric key pair that is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages, files, or other information that can then be decrypted with the corresponding private key. The user releases this key to the public who can use it to encrypt messages to be sent to the user and to verify the user's digital signature. Compare with private key.

Public key certificate

A digital document that is issued and digitally signed by the private key of a certificate authority (CA) and that binds an attribute of a subject to a public key.

Public (asymmetric) key cryptography

A type of cryptography that uses a pair of mathematically related cryptographic keys. The public key can be made available to anyone and can encrypt information or verify a digital signature. The private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public key infrastructure (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Also included in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

R**Radio frequency (RF)**

Any frequency within the electromagnetic spectrum associated with radio wave propagation. Many wireless communications technologies are based on RF, including radio, television, mobile phones, wireless networks and contactless payment cards and devices.

Radio frequency identification (RFID)

Technology that is used to transmit information about objects wirelessly, using radio waves. RFID technology is composed of 2 main pieces: the device that contains the data and the reader that captures such data. The device has a silicon chip and an antenna and the reader also has an antenna. The device is activated when put within range of the reader. The term RFID has been most commonly associated with tags used in supply chain applications in the manufacturing and retail industries.

Reader

Any device that communicates information or assists in communications from a card, token or other identity document and transmits the information to a host system, such as a control panel/processor or database for further action.

REAL ID Act

The REAL ID Act of 2005. Legislation intended to deter terrorism by establishing national standards for state-issued driver's licenses and non-driver's identification cards in addition to other key executables.

Registration

See identity registration.

Registration authority

A body given the responsibility of maintaining lists of codes under international standards and issuing new codes to those wishing to register them.

Response

A message returned by the integrated circuit chip to the terminal after the processing of a command message received by the chip.

RFID tag (labels)

Simple, low-cost and disposable electronic devices that are used to identify animals, track goods logistically and replace printed bar codes at retailers. RFID tags include an integrated circuit that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. There is little to no security on the RFID tag or during communication with the reader. Typical RFID tags can be easily read from distances of several inches (centimeters) to several yards (meters) to allow easy tracking of goods.

Role

The actions and activities assigned to or required or expected of a person or group.

Role-based access control (RBAC)

Access to resources based on a user's assigned role. Access permissions, which determine which resources can be accessed and the privileges in the context of that resource, are administratively associated with roles, and users are administratively assigned appropriate roles. Roles can be granted new permissions as new resources are incorporated, permissions can be revoked from roles as needed, and role assignments for users can be modified or removed as needed. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning the appropriate roles to the user, which simplifies common operations such as adding a user, or changing a user's department.

RSA

Refers to public/private key encryption technology that uses an algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman and that is owned and licensed by RSA Security.

S**Sarbanes-Oxley**

The Sarbanes-Oxley Act of 2002, which introduced changes to regulations that apply to financial practice and corporate governance for public companies. The Act introduced new rules that were intended "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."

Secret key

A key used with symmetric cryptographic techniques by a set of specified entities.

Secure hash algorithm (SHA)

One of the most popular hashing algorithms, designed for use with the Digital Signature Standard by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). SHA-1 produces a 160-bit hash.

Secure identity

The verifiable and exclusive right to use the identity information being presented by an individual to access a set of privileges.

Security attributes

Condition of use of objects in the ID card including stored data and data processing functions, expressed as a data element containing one or more access rules.

Seed

A random sequence of bits that is used in a cryptographic algorithm as the input to generate other, longer pseudo-random bit sequences.

SIM

Subscriber Identity Module. A SIM is the smart card that is included in GSM (Global System for Mobile Communications) mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.

Skimming

The practice of obtaining information from a data storage device without the owner's knowledge. Skimming is typically associated with magnetic stripe-based credit cards.

Smart card

A device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-

card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules used in GSM mobile phones, and USB-based tokens.

S/MIME

Secure Multipurpose Internet Mail Extensions. A protocol for exchanging digitally signed and/or encrypted mail.

Sniffing

The act of auditing or watching computer network traffic. Hackers may use sniffing programs to capture data that is being communicated on a network (e.g., usernames and passwords).

Specification

A set of documentation that reflects agreements on products, practices, or operations produced by one or more organizations (or groups of cooperating entities), some for internal usage only, others for use by groups of people, groups of companies, or an entire industry.

SSL

Secure Sockets Layer. SSL is a protocol used to transmit information on the Internet in encrypted form. SSL also ensures that the transmitted information is only accessible by the server that was intended to receive the information.

Standard

Specifications produced by accredited associations, such as ANSI, ISO, SIA, ETSI or NIST. In the United States the use of standards is typically optional and multiple standards can be developed on the same subject. In some countries, the use of existing standards may be required by law and the development of multiple standards on the same subject may be restricted.

Strong authentication

The use of two or more factors of authentication to prove an individual's identity. Factors would include some combination of something you know (a password or personal identification number that only you know), something you have (a physical item or token in your possession) and something you are (a unique physical quality or behavior that differentiates you from all other individuals).

Subject

A person, system or object with associated attributes.

Symmetric cryptographic technique

A cryptographic technique using the same secret key for both the originator's and the recipient's operation. (Without the secret key, it is computationally infeasible to compute either operation.)

Symmetric keys

Keys that are used for symmetric (secret) key cryptography. In a symmetric cryptographic system, the same secret key is used to perform both the cryptographic operation and its inverse (for example to encrypt and decrypt, or to create a message authentication code and to verify the code).

T

Template

Biometric data after it has been processed from its original representation (using a biometric feature extraction algorithm) into a form that can be used for automated matching purposes (using a biometric matching algorithm). Biometric data stored in a template format cannot be reconstructed into the original output image.

Token

A physical device that carries an individual's credentials. The device is typically small (for easy transport) and usually employs a variety of physical and/or logical mechanisms to protect against modifying legitimate credentials or producing fraudulent credentials. Examples of tokens include picture ID cards (e.g., state driver's licenses), smart cards, and USB devices.

Triple DES

A block cipher formed from the Data Encryption Standard (DES) cipher by using it three times.

Transitional products

As defined in NIST SP 800-73, products that meet the "Transitional" interface specification. Transitional products can be used as part of a migration strategy by Federal agencies that have already initiated a large-scale deployment of smart cards as identity badges.

Transponder

A wireless communications device that detects and responds to an RF signal.

U**Ultra-high frequency (UHF)**

Radio frequencies (RF) between 300 MHz and 3 GHz. When used in an RF-based identification system, the UHF frequency range is typically from 860 to 960 MHz.

Unique identifier

Any element or value which is guaranteed to be unique among a given group.

USB

Universal Serial Bus. A serial bus standard to interface devices.

V**Validation**

The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Verification

The process by which the question "is this person who the person claims to be?" is answered. This function requires a one-to-one match between presented identity information and identity information that is known to a system. See identity verification.

Vetting

The process of inspection, evaluation and adjudication of claims ensuring that people are who they claim to be before giving them authorization or rights to do something.

Vicinity card

See ISO/IEC 15693.

W**Web access management (WAM)**

Systems that replace the sign-on process on various web applications, typically using a plug-in on a front-end web server. The systems authenticate users once, and maintain that user's authentication state even as the user navigates between applications. These systems normally also define user groups and attach users to privileges on the managed systems. These systems provide effective access management and single sign-on to web applications. They do not, in general, support effective (or any) management of 'legacy' systems such as network operating systems, mainframes, client/server applications, and e-mail systems.

Wiegand strip

Technology widely used for physical access applications. The technology includes an interface, a signal, a 26-bit format, an electromagnetic effect, and a card technology. A Wiegand strip is the implementation of Wiegand technology on an ID credential.

Wired logic

A contactless card that has an electronic circuit that is designed for a specific function (e.g., security, authentication) without an embedded MCU.